2040 training

FUNDRAISING AND DATA PROTECTION

A survival guide for the uninitiated

Tim Turner

Contents

1 Introduction

Data Protection has a terrible reputation. For the tabloids, it's a bugbear, the excuse for any number of stupid and illogical decisions – whether it's hiding the name of an absconding prisoner or refusing to reveal the location of a missing cat, Data Protection always gets the blame. Most of what you read about Data Protection is nonsense, written by people who don't understand it and don't care. To make matters worse, there's a lot of DP guidance out there written by people with scarcely more rigour or understanding.

On the other hand, Data Protection law itself isn't that complex. It is based on a set of common sense principles. It presents six conditions that allow the use of personal data, and anyone who wants to process personal data must meet one of them. If you want to use sensitive data like health or sexuality, you must meet one of an additional set of conditions. You must set out what you want to do with personal data and why, and then you need to make decisions about what your justification is. The challenge is that the Data Protection doesn't tell you which one to choose, and for a charity or a fundraiser, some of the conditions only rarely apply. If there is a problem with Data Protection, it's that you need to think for yourself and then justify your decisions if things go sideways. The other thing you will almost certainly have to do is explain to the individual – the 'data subject' in the jargon – what you're doing with their data.

Data Protection might make you do things that you don't want to do. It might make it harder for you to do what you want to do. When people say DP is complex, they often mean that they don't like it. You will probably not raise a penny more for your cause because you read this guide. I'm not here to help you raise money because I don't know how to do that, and I'm not going to patronise you. The reason why so many organisations breach DP and PECR in the UK is because they make more money by doing so.

Data Protection treats charities in pretty much the same way as private companies. Asking people for donations, assessing whether a person is a likely donor, or maintaining records of supporters are seen as no different to marketing a product or service, profiling a customer, or maintaining a customer database. There is a single exemption for not-for-profit organisations, covering the technical area of sending a DP notification to the Information Commissioner. There are no exemptions covering marketing, fairness, security, enforcement or the use of volunteers. Parliament made no special provisions for charities – even if you think they should have, they didn't.

The regulator for Data Protection, the Information Commissioner, cannot grant an exemption from DP or PECR to any organisation or sector. Their enforcement can

be inconsistent, cautious, and reactive but if the ICO has never offered charities a free pass, despite the claims of some. They generally take action for three reasons – they receive lots of complaints about something, an organisation reports itself to the ICO, or there are big headlines about a Data Protection issue. Like it or not, although a variety of news organisations take an interest in data protection, the one that has consistently investigated DP issues over the past few years is the Daily Mail, which is how the current problem with charities got onto the ICO's radar.

The data protection principles have not changed since 1998 – not for charities or anyone else. The electronic marketing rules have not changed since 2003, and some elements (like the Telephone Preference Service) were in place before that. Various parties have issued misleading and unhelpful codes and documents – and the ICO's relatively consistent advice to charities has been consistently misinterpreted by those with an interest in doing so. Anyone who says that the action against charities in 2016 was based on a new interpretation of DP should show you evidence of what the law *used* to say, or guidance from the ICO from before 2015 about transparency that contradicts what they say now. They will have nothing.

Change *is* coming. It is true that a big Data Protection reform is expected in the UK in 2018 (based on the EU's General Data Protection Regulation). But even when that happens, the fundamentals will not change. Indeed, I've written this guide using those fundamentals as a bridge between the DPA and GDPR – I will mention GDPR especially when it significantly changes something you already have to do.

For a long time, there has been confusion about DP and PECR in the charity and fundraising sector. The Institute of Fundraising often gave (and still gives) flawed advice about Data Protection. Fundraising is often outsourced to private companies whose interests are as much in raising funds than complying with Data Protection. Compounding this problem was the fact that the Fundraising Standards Board received thousands of complaints about charity fundraising (particularly phone fundraising), and few, if any, of these complaints were passed on to the ICO.

Then Olive Cooke died. I am writing this in March 2017, and the fires started by the Daily Mail's incendiary coverage of both Cooke and Samuel Rae's stories are still burning. At the risk of alienating you before we even get started, I don't believe that the Mail are responsible for the flames. Some big charities didn't pay anywhere near enough attention to their legal responsibilities and some fundraisers either didn't know or didn't care what the law says. This meant that the entire sector – even the many who were doing things right – was doused in petrol. What the Mail did was to light a match. What the sector needs now is a fire extinguisher, not more fireworks. What it needs is compliance.

At the least, you have to comply with the law. There is a legitimate question about whether you want to go further than the law. The ICO would certainly prefer it and the Fundraising Regulator has published guidance full of *recommendations* rather than legal obligations. I am not going to talk about what you should do. What you *should* do is covered by ethics, and ethics are personal. I don't think it is unethical to shoplift from Sports Direct because of what I think of Mike Ashley. You might disagree because you think stealing is always unethical. However, I wouldn't expect my argument to work on a magistrate. Ethics cover things that you are allowed to do, and help you decide whether you *should* do them. The law is different. This is a terrible time to be bad at Data Protection. The stakes – in terms of reputation and enforcement – have never been higher.

The most important thing about Data Protection is that you think about it early. The GDPR makes it mandatory to adopt a Data Protection-by-Design approach, but the organisations who cope best with Data Protection only do so because they operate some version of this idea. The biggest advantage and the biggest problem I have is that I worked for the ICO at the start of the last decade. The two things I learned are not to be afraid of them, and that they are not infallible. It is acceptable, and sometimes advisable, to disagree with them, but only because you've got a better handle on how DP works in your situation than they have.

This guide was supposed to be complete in January 2017 but a variety of complications, personal and professional, delayed it. One factor was a fundraising conference held by the ICO and other regulators on 21st February, accompanied by guidance from ICO and the Fundraising Regulator. One interesting thread for the outsider was consistent criticism from attendees and observers that the ICO didn't appear to understand the sector, or the issues associated with fundraising. The ICO regulates every organisation that processes personal data, so they will never understand any sector as well as those who are part of it. The problem is that some people seemed to think that the ICO has to consider how important fundraising, and some specific techniques, are to the business model of charities when enforcing. To be blunt, they don't. The *importance* of your data processing to you is irrelevant. All ICO has to consider is whether your processing is lawful under DPA now, GDPR from next year. If you think DP is a problem, wait till you meet the GDPR, which is deliberately calibrated to give individuals greater control and autonomy, with transparency as a right.

Some of the risks you face are data protection compliance risks. The RSPCA and the British Heart Foundation found to their cost that sharing people's data without telling them that it is happening is a risk. Pharmacy 2 U found that selling customer data to people without telling them (especially selling the data to a variety of dodgy

people) was a risk. TalkTalk found that having an insecure website was a risk (especially as they could have fixed the website and yet they didn't). Each of these incidents resulted in fines from the Information Commissioner.

Some of the risks are practical risks – you might want to use volunteers to process your personal data, and ensuring an appropriate level of security to keep data safe might be too expensive. This isn't a data protection barrier – this is you wanting to do things without the resources you need. 'But we're a charity' isn't an excuse for allowing your data to be used by people who haven't been properly trained, or who are using their own insecure equipment.

Some of the risks are reputational – the Samaritans launched their 'Samaritans Radar' to monitor and assist troubled Twitter users, only to pull it because of a backlash from Samaritans users. Samaritans Radar had a multiplicity of Data Protection problems, chief among them legal advice they claimed said DP didn't apply to the scheme. The DP issues didn't cause the damage. The perception among people who rang their helpline that the Samaritans had breached their trust, invading their privacy in a way that they didn't expect was what proved so harmful. The Samaritans received no enforcement action by the Information Commissioner (to their credit, they pulled Radar once they saw the reaction). Nevertheless, I've met Samaritans' users and donors who still don't trust the charity now, even though the Radar incident happened in 2014.

You understand charities and fundraising – what I want you to do develop your own take on how Data Protection works in that context, think it through, and apply it. Then, if you're challenged by the ICO, stand your ground. On any of the grey areas, you don't have to agree with my take on how DP works. If we ever meet, we'll be friends forever if you don't agree with me. I love an argument about Data Protection because it helps me to understand the legislation better (and because I love an argument). And in the real world, facing the ICO, if you can explain your thinking based on what the DPA says, you'll be in a stronger position to defend your actions than if you just say that the DPA is wrong.

Tim Turner
March 2017

NB: Throughout this guide, you will see 'actually asked questions' – these are genuine questions submitted to me by charity representatives before I put this guide together

2 Ten essential things you need to know about data protection

1) There is no significant charity exemption to data protection or marketing law. Maybe there should be. There isn't.

2) The ends never legalise the means.

3) If a donor or other individual does not understand what you are doing with their personal data, the practical effect is that you can't do it, whatever it is. The same is true for consent – if a person doesn't understand what you're doing, you can't argue that they have consented to it.

4) You don't need consent for every use of personal data, but if you don't have consent, you need to know what other justification you have that allows you to use the data. The other reasons are specifically set out in the Data Protection Act and the GDPR.

5) You cannot assume consent. Failure to opt-out is not consent. Silence is not consent. Previous support is not consent. A donation I give you today is not consent for something tomorrow.

6) Volunteers are no different to employees; they must be trained and equipped to protect data. There is no volunteer exemption. Using volunteers is a choice you have made, and you are responsible for ensuring that you manage the risks adequately.

7) If you contract out any work to an agency or contractor, you are wholly responsible for what they do, unless they steal your personal data or otherwise use it for their own purposes.

8) Personal data available in the public domain is still personal data and Data Protection still applies to it.

9) There are specific rules for consent over the method of communicating fundraising and other direct marketing communications. Beyond that, you have to decide whether you need consent or whether some other condition applies.

10) Never accept data protection advice from the Institute of Fundraising.

3 The Information Commissioner

There are two pieces of legislation you need to be aware of – the Data Protection Act 1998 (DPA from now on) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR from now on). The DPA covers all processing of personal data, regards of the purpose; PECR covers a variety of communications-related activities, but it includes specific rules for electronic direct marketing. The DPA will be replaced in the UK in May 2018 by the General Data Protection Regulation (GDPR), a pan-EU data protection law the government has decided will apply despite the Brexit vote. It is largely an evolution of the current legislation, but some of it makes mainstream good practice into a requirement, and it beefs up the rights considerably.

Both pieces of legislation are enforced by the Information Commissioner (also known as the Information Commissioner's Office or ICO), an independent regulator based in Wilmslow in Cheshire. The current incumbent is Elizabeth Denham, a former privacy commissioner from Canada. Unlike most of her predecessors, she has significant privacy and information rights experience. The Information Commissioner did not write and cannot change the law – only Parliament can do that. If you want the law to say something different, write to your MP or lobby the Department for Culture, Media and Sport – the ICO can do nothing.

The ICO does several things that you need to know about:

Guidance: ICO guidance is designed to assist you to comply, but the ICO's guidance is a mixed bag. Guidance is not law, and if you believe that ICO guidance is wrong (or if you can see an equally compliant alternative), you don't have to do what they say. It is worth saying that ICO guidance sometimes goes further than what the law requires while not making it clear that this is the case. If you know that you are not following their guidance, be sure that you can show that your interpretation of Data Protection law is correct. Any other considerations – the inconvenience of what they're advising, or the negative effect on what you're doing, are irrelevant. Build your case on what the DPA / GDPR or PECR say if you want to follow an alternative path.

Assessments: ICO can deal with individual complaints from members of the public – their decision is known as an 'assessment'. The assessment process is flawed from the complainant's perspective because there are no immediate consequences if you ignore the ICO's assessment. If you do not agree with it, nothing happens automatically. Clearly, there is no better way to get on the ICO's radar than to ignore the outcome of an assessment, and an adverse assessment will be useful to the complainant if they decide to sue you.

Enforcement Notice: The Enforcement Notice is one of the ICO's two significant powers under the DPA. If they decide that you are breaching any part of the Act, they can order you to take any action necessary to rectify the breach. This can be anything from an order to answer an ignored subject access request to a demand to train more staff (a measure they believe is required to comply with the security principle). In 2016, the ICO issued a multi-part enforcement notice on the Alzheimer's Society, requiring a wide range of measures covering retention, training, security of devices and the use of volunteers and data processors, which is one of the most demanding notices of its kind ever issued.

An enforcement notice can only be served if the breach is ongoing – once the organisation has rectified the problem, the enforcement notice cannot be served. Before serving the final notice, the ICO is highly likely to give the organisation the opportunity to comply voluntarily. If an Enforcement Notice is served, the organisation has either refused to comply, or said that they cannot comply with what the ICO requires. If the organisation does not appeal the notice, and does not comply within the set timescale, the ICO can prosecute them.

Civil Monetary Penalty (CMP)

The CMP is a punishment. Even if the breach has been rectified by the time the CMP is served, it is still valid. Enforcement notices are generally served when the breach is serious, but the criteria for serving a CMP are stricter. The breach must be serious, it must be likely to cause damage or distress to data subjects, and finally, the breach must be deliberate (the organisation knew their actions would breach an aspect of Data Protection, or deliberately set out to breach the DPA) or the data controller knew or ought to have known about the potential breach and failed to take appropriate measures to prevent the breach.

The ICO doesn't often claim that the organisation deliberately breached the DPA, but the CMPs served on the RSPCA and the British Heart Foundation were characterised as deliberate, in the sense that the charities consciously did not inform subjects how their data was being used, rather than acting recklessly or ignorantly.

Undertaking: The undertaking is the joker in the pack. Their announcement often feels a punitive step, and they always require the organisation to take concrete action. However, the ICO doesn't have a specific power to serve undertakings – they're not mentioned in the DPA, and there is no formal sanction if an organisation signs an undertaking and then fails to comply with it. The ICO *asks* the organisation to sign the undertaking, and they agree. There is an element of naming and shaming in the use of the undertaking, and the ICO seems to use them as a kind of

soft enforcement notice where the organisation is willing to cooperate. My problem with this is that if an enforcement notice isn't required because the organisation is willing to do whatever it is the ICO wants them to do, I don't see why the undertaking is necessary. It seems like more of a PR exercise than anything else.

In 2016, British Red Cross and Age International signed undertakings to renew consent every 24 months, a step that the ICO confirmed went beyond what is legally required – the current Commissioner described them as 'best practice undertakings', the reverse of the atmosphere of punishment that the ICO usually wants undertakings to evoke. Whether the ICO will issue any more 'best practice' undertakings remains to be seen.

A few words about the ICO helpline: there is arguably some value in the ICO operating a helpline for the public, answering questions about how to make subject access requests or how to make a complaint to the ICO. The helpline is almost no use for the data controller unless the question being asked is of a rudimentary variety. If your question goes beyond 'do we have to answer a subject access request?' or 'am I covered by the Data Protection Act?', there is little point in asking the helpline. The staff on the helpline do their best but they are likely to sit on the fence, and the calls are not recorded, so even if you get something approaching concrete advice from them (you won't), you will have no evidence that the advice was ever provided.

Other powers: the ICO can apply for a warrant to gain access to premises and seize documents or equipment. To my knowledge, this has never been necessary in a charity or fundraising case – they seem to use warrants to catch PPI spammers in the act. However, they also have a power to issue an Information Notice, which allows them to demand access to any information they require to carry out an investigation. Like an Enforcement Notice, an Information Notice is only likely to be issued on an organisation that has refused to provide information voluntarily, and also like an Enforcement Notice, an organisation that refuses to comply with one can be prosecuted.

GDPR Powers: the ICO should get a wide range of new powers under the GDPR, but it's hard to know how they will be used until the GDPR comes into force. It is unlikely to have escaped your notice that GDPR carries maximum penalties of €20,000,000 or 4% of an organisation's annual turnover. However, I believe that a cautious regulator like the ICO is unlikely to issue a penalty that even approaches that maximum figure.

4 Data Protection fundamentals

4.1 Start from the right place

This section is the bulk of my advice to you.

If you haven't thought about the impact of Data Protection on your processing from the beginning, you will be on the back foot if anything goes wrong. If you can make a solid case that what you're doing complies by referring to what the DPA / GDPR says, ICO staff may be reluctant to substitute their judgment for yours in the event of complaint. On the other hand, it will be very difficult for you to work backwards if you didn't do your research and think through your argument through at the outset. If your explanation is just post-rationalisation after something went wrong, it's unlikely that you will get anywhere.

Three commonly-used arguments never work – cast them from your mind:

- We've always done it this way
- Everyone else does it
- We'll lose support / money if we do it your way

Everything you say needs to be connected directly to the DPA or the GDPR. But remember that Data Protection is principles-based – this is why DP people say 'it depends' so often.

Three crucial definitions

- Data subject – the data subject is the person the data is about

- Data controller – the data controller is the organisation that 'determines the purposes', that decides to gather and use the information

- Data processor – the data processor carries out specific tasks on behalf of the data controller under contract and is generally not liable for enforcement if it does what it is told to do by the data controller. There must be a binding contract; if there is not, now and under the GDPR, it's a breach for which the controller is liable

  If a controller like a charity or university hires a company to carry out wealth screening or make telephone calls on their behalf, that organisation is a data processor. If the company *already holds* the data (hypothetically, let's say they hold a database of 100,000s of high net-

worth individuals), you are both data controllers. If you buy personal data from a company, they are a data controller for the purposes of selling the data, and you are a data controller once you buy it.

Personal data

The DPA and GDPR apply to a specific type of information. Both of them define personal data as data about or relating to a living, identifiable, individual. The information must allow you to identify the person either by itself, or in combination with other information that might be available to you. If you know who the person is, or can work out who they are, DP applies to what you're doing now and under GDPR.

If you're using data that identifies someone, it allows you to distinguish one individual from another, then that data is personal data. If the information is genuinely anonymous i.e. you do not know who the information is about, DP does not apply to what you are doing. Bear in mind, anonymous information has to survive the attention of whoever might have access to the data – if you publish an anonymous case study on a website, it should not be possible for someone to take the case study and work out who it relates to.

The DPA definition of personal data is data that relates to a living individual who can be identified from the data itself or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

The GDPR goes a bit further:

- Any information relating to an identified or identifiable natural person (a natural person is an individual rather than a legal person like a company)
- 'data subject' = identifiable person who can be identified by an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to person's physical, physiological, genetic, mental, economic, cultural or social identity

Data in the public domain

Many people struggle to reconcile themselves with the fact that so much personal data is in the public domain, and yet the perception surrounding data protection is that it exists solely to lock up information and keep it secret. The problem starts with the terrible name: 'data protection'. It's inaccurate, because the purpose of Data Protection is to regulate and control how personal data is used, rather than

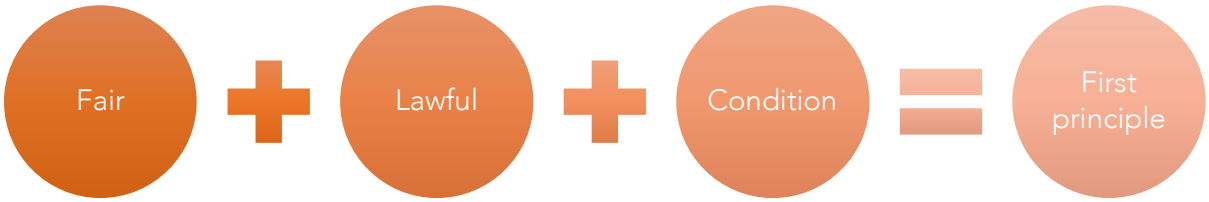
keep it locked away. Security is a powerful element of the legislation, but it's not the only thing.

Data in the public domain is not exempt from the DPA or the GDPR – look for any reference to public domain data being excluded, and you won't find it. In a roundabout way, the Act confirms that personal data in the public domain is still covered. The DPA defines certain information as being sensitive data: racial or ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health or condition, sexual life, information about criminal convictions and any criminal proceedings against the subject. The use of all personal data requires the organisation to meet one of a set of conditions (see part 4.5 below), but for sensitive data, the requirements are stricter, with a second, more narrowly drawn set of conditions. One of them is that the subject has willingly put their data into the public domain. If the assumptions about public data were correct, this provision would not be necessary.

Moreover, the GDPR makes clear that people need to be told if their information has been obtained from publicly accessible sources – again, this would not be required if Data Protection did not apply to publicly available data.

4.2 The first principle

The basis of Data Protection is the first and second principle. The first principle requires three things.



To comply with the first principle, you need to set out the purposes for processing personal data. Talk to your colleagues about what you're doing. Get a clear idea of what you're doing with personal data and why. If you can't describe the purpose or purposes neatly and simply at the outset, you're stuffed. Key questions about how you comply will be impossible to answer – what condition (see below) you rely on, how long you keep data for, how much of it you need – all of this is dependent on the purpose for which you are processing data.

What is your purpose?

The second DP principle requires two things – an administrative task (sending a notification describing your processing to the Information Commissioner) and a compliance tasks. Let's ignore notification because it is effectively abolished by the GDPR, and concentrate on the second part – compatibility.

The DPA says that personal data shall not be processed in any manner incompatible with the controller's "*specified and lawful purposes*". The GDPR is almost identical – data shall be "*further processed in a manner that is incompatible with those purposes*". The GDPR purposes must be "*specified, explicit and legitimate*". Once again, you must set out your purposes clearly and unambiguously, and you can't just say 'fundraising purposes', when that could cover a huge variety of data uses. The discipline of clearly identifying your purposes at the outset is one of the most useful things you can do, and you must break down 'fundraising purposes' into its constituent parts.

If you want to use data for a second purpose, you will need a persuasive case that what you're doing is not in conflict with the original purpose. If it can be said to be incompatible with the original purpose, you're sunk. You cannot use the data; at best, you must go back to the beginning and satisfy the first principle and conditions again for what is a new purpose. It is highly likely to be unfair to try to repurpose information for a new, incompatible purpose.

Write your purposes down, like this:

a) We want to maintain a list of people who have donated to us before, so that we can contact them to ask them to do so again
b) We want to maintain a list of people who have explicitly told us that they don't want to contact us again
c) We want to use (a) to research the donors' financial background using public sources to work out what kind of approach to make to them
d) We want to use (a) to research the donor's financial background, and we want to pay a company to do the research for us
e) We want to buy data from a third party to make sure that (b) is up to date
f) We want to buy data from a third party to create a list of people who have never donated to us, so that we can contact them and ask them to donate for the first time
g) We want to claim gift aid on a person's donations
h) We want to keep their information up to date

And so on. Unless you want to steal data or use it in a misleading or actively prejudicial way, it's unlikely that any purpose will be ruled out because Data

Protection doesn't have a list of proscribed purposes. You define your objective, and how you want to use personal data to achieve that objective. Always consider whether what you want to do is necessary and proportionate, and be mindful of the risks. Try to address those risks in the way you design your processing (i.e. if data is obtained from a third party, ensure that you do your due diligence).

The ICO's recently issued guidance on Fundraising and Data Protection caused some raised eyebrows when it touched on appending – the practice of acquiring additional data from a third party where it was not provided by the subject. Some charities argued that the 4th Data Protection principle requires them to keep data accurate and up to date, but the problem here is that only up to date "where necessary". If the purpose is a record of a previous donation, the data is accurate even if it goes out of date, but it only needs to be correct for that moment in time. If the purpose is Gift Aid, the organisation must tell the person that it needs up to date information, and will obtain it from a third party if it is not available from the subject.

Once you've identified your purposes, the first DP principle requires you to answer three questions. The questions survive intact into the GDPR.

- Is the processing lawful?
- Is the processing fair?
- Have we met a condition?

4.3 Is the processing lawful?

You can't break other laws in the way that you use personal data, so you have to look at any other laws relevant to your organisation or sector that might affect how you're using personal data. The problem here is that you need to understand the legal framework that applies to your charity. When I was a local government data protection officer, I knew that we had to comply with the Human Rights Act. This meant that if we obtained data in a way that breached people's privacy (for example, when obtaining photographs in their house), it would also have been a breach of the first Data Protection principle. The problem with this part of the Data Protection Act is that it requires you to understand the *other* laws that apply to your organisation. I can list laws relevant to local government and the NHS because I worked in both sectors – the challenge for you is to understand whether any laws relevant to what you do impact on the way you gather data.

4.4 Is the processing fair?

There are two ways that you have to deal with fairness. The first is harder conceptually and the second is harder practically.

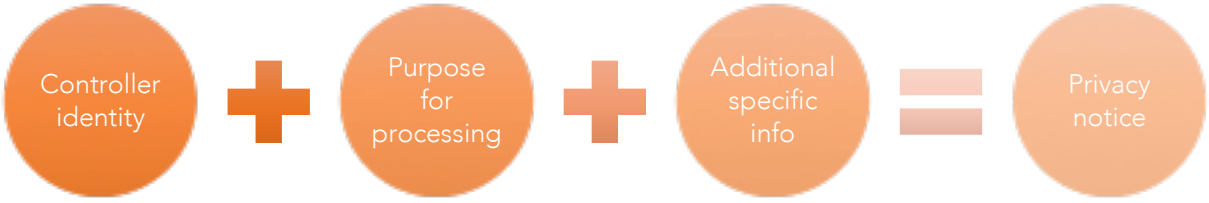
Fair in the general sense

Your processing must be 'fair'. Look it up in the dictionary if you're not sure what 'fair' means. This isn't as dismissive as it sounds; tribunals and courts sometimes use the dictionary as a starting point. My dictionary says that fair means "*free from discrimination, dishonesty etc.; just; impartial*" or "*in conformity with rules and standards*". Data Protection is not a science, and it isn't unreasonable for the Commissioner, or others, to demand an ethical aspect to data processing. It's why NHS and other bodies have a Caldicott Guardian whose role is not to ask whether data processing is legal, but whether it is right – not can we do this, but should we do it. There's an argument that the duty of confidentiality owed by health professionals to patients makes the Caldicott role more necessary than in other sectors, but I would dispute this. If you're not asking whether something is ethical as part of your Data Protection compliance, you're doing it incorrectly because you're not considering the wider fairness issues. As the ICO's new charity guidance says: "*processing does not become fair just because you tell the person it will happen*".

You have to decide what you think is fair to the data subjects. If challenged, either by the subjects, by the Information Commissioner or the courts, you will need to set how you have dealt with fairness. It will be much harder to do this if you have not thought about it in advance. A common place to start – which is corny but effective – is to ask yourself, how would I feel if this was my data? How would I feel if it was my Granny's data? How would I feel if it was my kids' data? This test is subjective, but there's something to be said for listening to your conscience and your gut when considering the wider meaning of fairness.

Here's an example – I spoke to several DP professionals, and one of them came up with the following scenario. *If I buy a charity raffle ticket, it is unfair for the charity to do any form of wealth screening on me without giving me a choice – they should either ask for consent or they should give me an opt-out.* They said that absence of an opt-out was unfair, even if technically, the legitimate interests condition doesn't require it. I don't agree with this, though I do agree that it's fairer and less prejudicial with the opt-out than without it. The point is, neither of us can say that we're right: it's a matter of opinion. If you're not going to give people a choice, you should be able to explain why it's fair not to give people a choice.

Fair in the sense of transparent



A sausage probably tastes better if you don't see what goes into it – similarly, some fundraising techniques, especially those involving research or profiling, are probably more effective if the target isn't aware of why and how they came to be a target. One venerated fundraiser scolded me for suggesting that prospective donors should be informed about how their data was obtained, and why they have been approached. But this collides with the legal reality: if you research people without telling them, it's a breach of DPA and GDPR.

The fundraising sector knows about and understands profiling and research. Many were aware of the Reciprocate data sharing scheme or similar initiatives, secret participation in which was partly the cause of the ICO's action against the RSPCA and the British Heart Foundation. But in my experience, the public had no idea that fundraisers, particularly charity fundraisers, used as much profiling and research as they do. I've used it as an example on most of the Data Protection courses I have run in the past couple of years, and the delegates are gobsmacked. Most of the people I train are not privacy obsessives, they're just ordinary folk doing a job that involves personal data.

Few charities have ever been transparent about profiling and research, and I believe this is because it's hard to describe it without it sounding weird. You are welcome to disagree, but finding language to describe it accurately without being euphemistic and without making it sound weird is a challenge for the fundraising sector at the moment. It is a challenge made all the more difficult for the fact that the process has

been done back to front – organisations have enjoyed the benefits of research without the awkwardness of explaining it to those who have been researched.

My advice is as follows (bolstered by the ICO's enforcement action). Your privacy notice should contain clear references to the following:

- Data sharing with another organisation (regardless of whether data is sold or exchanged for free)
- Research, regardless of whether data is obtained from the public domain, or a publicly accessible source. By research, I mean attempting to find out any information about a person's financial position, property, previous donations or their propensity for giving
- Any other profiling, research or screening, which may include age, interests, health, or ethical or similar assessments (some consultants offer a service of assessing potential ethical conflicts created by a donation from a prospective or actual donor)
- Acquiring data from third parties – this includes the details of prospective donors, acquiring data to flesh out existing or prospective donor records

These references should be in plain language without waffle.

If you don't want to tell a donor or volunteer about one of the purposes for processing their data, ask yourself why. If it is uncomfortable or awkward for you to explain it, it's almost certainly something that fairness demands they understand. If you cannot find a simple, straightforward way of explaining it, you can't do it. The person doesn't need to understand the software you're using, they need to understand the purpose you're using it for. If you can explain why you think it's fair not to tell people about the above purposes, contact me using the email address at the back of this guide.

However you negotiate the territory of general fairness, the second meaning of fairness is more concrete. You must provide specific information to the individual, regardless of whether you receive their data directly from them or from a third party. Under the DPA, you must tell them who you are, set out the purposes for which their data will be used, and you must give them any other information that is necessary to make the processing fair. Arguably, you should set out all the purposes, but the ICO says that if a purpose is obvious, you might be able to rely on the idea of 'reasonable expectations'.

Do we have to tell them at all?

The concept of 'reasonable expectations' isn't mentioned in the DPA or GDPR, but it's how ICO answers the question of whether fair processing information should be provided directly to the subject, or made available somewhere. Their Code of Practice on privacy notices states: "*If it is reasonable for someone to expect that you will use their information for an intended purpose, you are less likely to need to actively explain it to them and can instead make privacy information available if they look for it.*" GDPR helpfully says that if the person has the information already (e.g. you have told them before, or someone else has told them), you don't need to tell them again.

You don't need to tell people what you're doing if it would represent a disproportionate effort. The effort clearly has to be balanced against the impact that the processing will have on them – Article 14(5)(b) of the GDPR sees disproportionate effort as applying to archiving in the public interest or statistical use. In other words, it's likely that disproportionate effort only applies when the processing will have little direct impact on the subject. The same article also allows you not to tell the person if transparency makes achieving your objective impossible, or serious impairs those objectives. This may sound appealing, except that in these circumstances, you must ensure that a description of what you're doing is publicly accessible, and take measures to protect the individual's rights, freedoms and legitimate interests.

Where you are consciously not telling people that their data is being processed, it's impossible for them to exercise their rights. The thrust of the ICO's guidance in this area has always emphasised transparency over processing that is unexpected or objectionable. My rights of access, to object to direct marketing, to rectification and to erasure of my data are meaningless if I don't know that my data is being processed. Therefore, it has always made sense for the ICO to emphasise transparency over the unexpected. Many fundraisers claim that high net-worth individuals expect research before an approach – here is an opportunity for them to roll the dice on that proposition. If it's true, the target will not complain when they find out how their data has been used.

The language you should use

The average privacy policy or privacy notice is long-winded, technical and filled with waffle and euphemism. Lawyers often get the blame for this, but it's just as often a data protection officer who thinks that a privacy notice should be written like a legal contract, ticking a box for the sake of ticking a box. Many privacy notices and policies are useless because the people writing them don't know what they are for,

and so they fill endless pages with guff. Charities and other fundraisers are by no means the worst offenders here – pick any price comparison website and you will find T&Cs that make the average charity notice look like a paragon of transparency.

The best privacy notices are as short as they can be, written in language that is plain to the point of bluntness, and highlighting the most surprising and unexpected things that you are doing. You might be doing lots of things, and writing a short, simple privacy policy might seem impossible. I'm not sure I believe that, but the ICO offers two solutions to the problem, both of which have merit.

First, the ICO suggests a 'layered approach', which means having a short list of bullet-pointed headlines, with more detail provided to those who want it elsewhere. The classic example is to have a leaflet or email with the bullet points, with a link to a more detailed version on your website. The danger with a layered approach is the temptation to bury the more awkward purposes on the website version, with the headlines giving a more sanitised picture. In the end, you will get no credit if you bury difficult or surprising purposes somewhere that the person won't see them.

The subject doesn't need to know how important Data Protection is to you. They don't need to know – in most cases – how you're processing the data or what security you're using. They need to know why you're using their data, what the purposes for processing their data are.

Second, the ICO's GDPR-inflected privacy notices code recommends 'just-in-time' notices, an attempt to get away from the one-size-fits-all approach that many organisations take to fair processing. Many try to deal with fair processing in one hit – even if I am just browsing a company's website, the privacy notice tries to tell me about home delivery, complaints, their comments policy and how important Data Protection is to them. At that point, what I need to know is what cookies they're using, with what effect.

Clarity of language

I looked at a Big Name Charity's donation page on their website. The form asks for name and address, email and so on. By the email address is a tick box, and the following text: *Keep me up to date with Big Name Charity's projects and fundraising activities by email (we will not share your data and you can unsubscribe at any time).*

On the face of it, this is commendable: simple language, a straightforward choice to opt into marketing. Of course, if Big Name Charity (BNC) is processing my data for any purpose other than administering my donation or marketing that I have opted

into, it would not be fair, because I would not be aware of it. But what's this? At the bottom of the page is a link to 'Privacy & security'. The donation page makes no reference to this, but I looked at it anyway. Here, we have more detail, most of it innocuous, but in the middle, almost as an afterthought is this, which I have separated into two sentences:

In order to ensure that the data we hold about you is accurate and up to date, we may occasionally use information sources that are in the public domain to verify your details, such as address and telephone number.

Having said that the data is being processed for accuracy purposes, the only thing that BNC can use the data for is ensuring data that it already has is still accurate. If a donor or supporter has not supplied their address or phone number, it will be unfair for BNC to buy it from someone else in this instance. It will be even more unfair to contact a person using a phone number they haven't supplied because again, as no reference is made to that in the privacy policy.

The second sentence is terrible: *Sometimes we may use third parties to supplement the information that we hold as we only want to send you information which we believe you will be interested in.*

If this is BNC's way of saying that it carries out profiling or prospect research, it's vague to the point of being unfair, especially if it refers to any kind of wealth screening or financial analysis. It's not clear what the source of the information is, how it will be obtained. If BNC think they have consent for this, they don't, because the consent is not informed. If they think they have met the legitimate interests condition, I'm equally sceptical – how can their processing be legitimate if it is not fair, if the true purpose has been obscured?

Actually asked question: *Do I need to say 'we use publicly available sources to learn more about you' or do I need to be more specific i.e. 'we may use information filed at Companies House, written in newspapers etc."?*
Answer: At the moment, I think the former is enough – it's not woolly or vague and clearly indicates what is happening. The GDPR talks about "*from which source the personal data originate, and if applicable, whether it came from publicly accessible sources*", so here, I think a judgment call is necessary

Actually asked question: *Do we need people to consent to our privacy notice in its entirety?*
Answer: This is slightly the wrong question. The purpose of the privacy notice is to inform a person about the purposes for using their data (and under GDPR, a wider variety of issues). You might want a person to sign to say that they understand the privacy notice, but consent and privacy notices, while linked, are separate issues. The first question is whether you have told people the purposes for using their data. The second question is whether you are using the consent condition, or another one.

Actually asked question: *A donor has sent us an email suggesting we approach his friend for a donation. The friend refuses and demands to know where we got his name from. Do we need to ask the donor for permission to tell his friend? Do we need to tell the friend anything? If the donor says 'Don't tell him it was me' what should we tell the friend? Or, should we not approach the friend in the first place, until we have consent from the donor that we can name him as the source of the friend's name.*
Answer: There are two issues here – you have to ensure that method of contacting the friend is lawful, which means squaring it with PECR (i.e. post is good, but email is only possible with the friend's consent). The second issue is the fact that the subject (i.e. the friend) has a right to know the source of their data under the right of subject access. The donor cannot expect confidentiality in this situation, having opened up someone else to marketing they may not have wanted.

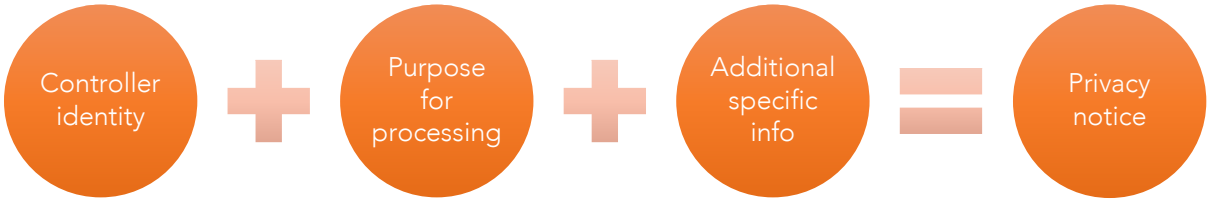
Do we provide a privacy notice, or make available on our website?

Here you have a quandary. The DPA says that fair processing information should be '*provided*' to the data subject, or it should be '*made readily available*' to them. To me, the distinction clearly allows for two options. '*Provide*' means you give them the information directly, while '*make available*' leans more towards making sure that the information is in an obvious place for people who want to see it. *The DPA doesn't tell you which*; you must decide and then justify your decision if you're not going to tell the subject directly. GDPR just uses the word 'provide'.

GDPR and additional information

The GDPR will make a difference to this part of the process, requiring considerably more detail to be available to the individual. The GDPR puts fair processing into a more coherent framework, with the individual told how their data is being used, what legal basis (i.e. condition) is being used to process the data, and then what

their rights are. GDPR gives the person the tools to understand and then challenge the way in which their data is used. You need to be ready for this.



The third element changes radically. Instead of you deciding what additional information you think the person needs, the GDPR sets out a detailed list of information that you must provide – this includes the legal basis for processing the data, the retention period for the data, and (if you obtained the data from a third party), the source of the information. If you have obtained the data from a wealth screening contractor or the public domain, you would need to explain this.

Moreover, the GDPR changes the purpose of fair processing. Under the DPA, fair processing is important, but technically, it is one of the responsibilities of the Data Controller, a job you need to do (well). GDPR classifies fair processing as one of the data subject's rights. If you want to process my data, I have a right to know why, and how long you'll process it for. I think this is a big change, and it hasn't had enough attention.

Actually asked question: *can I use data from Companies House to identify where a potential donor works and the contact them by post?*
Can I use the Sunday Times Rich List to identify graduates / potential donors?
Can I search directories like Who's Who lists and then contact them?
Answer: Yes, but you would need to tell them (in the first contact) how you obtained their data – consent not required because you could rely on legitimate interests. NB this answer only works for post or corporate subscriber emails (see PECR section for more)

Actually asked question: *can I set up a Google search for someone?*
Answer: Yes – it would be compliant if you informed the person when it was set up. If you do not tell them immediately, the only justification that you are likely to have – given that you are technically processing their data – would be that it is disproportionate effort. I think this argument only hangs together if the Google search is the only thing you have, and you would still need to tell them how you obtained their data when you contacted them. If you had an ongoing, especially automatic Google search running as well as other data, you have to consider that the whole is greater than sum of its parts – you have created new data.

4.5 Conditions for processing data

There are six conditions to justify the processing of personal data, found in Schedule 2 of the DPA, and Article 6 of the GDPR. You must satisfy one of them. This is not optional, or good practice. If you cannot say you have met one of these conditions, you're sunk. Do not pass Go, do not collect £200. Some of them are easier than others to use, you decide which one applies.

Most of the conditions do not apply to charity work in general and fundraising in particular – here's a quick summary about why.

Contracts – especially in fundraising, it is unlikely that there will be any kind of binding contract between the fundraiser and the donor / prospective donor. You might have something approaching a contract for organised sponsored events (especially ones with health and safety implications), but the only necessary processing would be to make that contract work. You wouldn't be able to make marketing a requirement of the contract, or assume that you can send marketing because the person signed the contract.

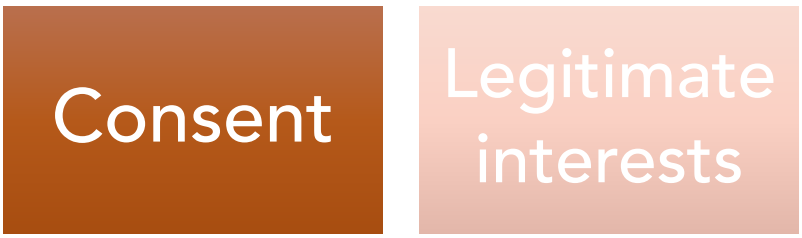
Legal obligation – it's unlikely that any law requires you to do any fundraising or activities associated with fundraising; if you can find one, go ahead. As above, you might organise an event (perhaps a sponsored bungee jump) with health and safety implications, or you may be required to comply with tax laws. If the law says you must process personal data, or you cannot comply with a specific law without processing personal data, go ahead. The crucial question is always the same; which law are you quoting, and what exactly does it require you to do?

Vital interests – vital interests condition works only if someone is at immediate risk of death (it's been argued that vital interests might cover serious physical risk, but the GDPR suggests that it applies only to life or death situation).

Official functions / administration of justice / public interest: this long, detailed condition applies to necessary for administering justice, or for exercising statutory, governmental, or other public functions. Again, for this to apply, you need to identify a specific law or source of official authority. The condition also includes a rather ponderous definition of tasks carried out in the public interest: "*the exercise of any other functions of a public nature exercised in the public interest by any person*". The mess is somewhat cleared up by the GDPR, which settles on a much more simpler formulation – exercise of official authority for the first part, and a task carried out in the public interest for the second. I am certain some fundraiser will argue that raising charitable funds is a task carried out in the public interest, and I am equally certain that it will come to nothing.

GDPR also creates a problem for universities and other public bodies that carry out fundraising – the use of legitimate interests is forbidden for a public body carrying out its tasks.

That leaves you with two choices (or for a post-GDPR public body, one):



4.6 Consent

Consent is not defined by the DPA itself, something which has slightly hampered the legislation ever since it started. However, if something in the DPA is ambiguous or uncertain, clarification might be found in the EU Directive on which it is based. The Directive has a much clearer definition, and this is the one that the ICO and the

courts rely on. The Directive definition of consent is "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*"

Freely given – the person must be given a free choice in the first place, and they must be able to change their minds at any time. You can't trick someone into giving consent and when they tell you to stop, you must stop.

Specific – the processing that they are agreeing to must be clear – what marketing are they going to receive? Who will it be from? Asking someone to agree for their details to be shared with "carefully selected third parties" isn't specific. If you want to do wealth screening with consent, asking the person to agree to 'fundraising purposes' isn't specific.

Informed – if the person doesn't properly understand how their data is going to be used, then the consent is not valid. You have to spell out what they're agreeing to, in language that they understand. You cannot bury the purpose in terms and conditions that the person might not read. The language should be clear, unambiguous and not euphemistic. Yes, this is the third time I have used the word 'euphemistic'. It is not an accident.

4.7 Can consent be opt-out or does it have to be opt-in?

There are plenty of people in my business who will tell you that opt-out is a perfectly reasonable way of getting consent. Even the ICO's current guidance on direct marketing suggests it's possible. But hold your horses; look at what the ICO actually says: "*organisations cannot assume consent from a failure to opt out unless this is part of a positive step such as signing up to a service or completing a transaction*". The most certain way to get consent is a tick box, a box to place a signature, or something else that allows the subject to say 'yes'. However, as the ICO notes, there are other methods. If a person fills in their name and address in a form clearly designed to send out a brochure, you can reasonably infer consent to send them the brochure. My advice is to pop a tick-box on the bottom to put the matter beyond doubt, but the ICO is clearly a bit more open-minded and they're the ones who can fine you.

Here's what you can't do:

- Untick this box
- Tick this box if you do not want to receive marketing (especially if the marketing is email or text)
- Text STOP

- By giving us your details for [unrelated thing], you agree to receive emails

Let's go back to the bit I quoted from the Directive. Freely "**given**", and "**signifies his agreement**". An opt-out is the absence of consent – you're assuming consent, it hasn't been given, there is no activity that signifies agreement. Opt-out or pre-ticked boxes don't get you consent.

4.8 What about implied consent?

There is no such thing – in Data Protection at least – as implied consent; it's not mentioned anywhere in the Act or Directive. You cannot say that because I bought a raffle ticket, or gave you a donation, that there is an implication of consent for marketing, fundraising or whatever else. Besides, how can consent be specific and informed if you're inferring from some other action that the person has consented? You can't get consent unless you ask for it specifically, and you can't get consent unless the person gives to you. The ICO's recent guidance on GDPR consent confirms this without any hint of ambiguity: "*Consent requires a positive opt-in*"

4.9 How long does consent last?

The ICO's consent guidance says "*There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.*" This is an interesting observation because in 2016, the ICO asked the British Red Cross and Age International to sign undertakings that committed them to refreshing consent every 2 years. Refreshing consent is plainly what the ICO considers to be good practice, and 2 years does not sound like an unreasonable time, but they acknowledged that the undertakings went beyond what the law requires.

The real limit of how long consent lasts is what you tell the person at the start. If you give the individual the impression that they are consenting for a limited time campaign, their consent ends when the campaign does. If you persuade the person to opt into a long-term relationship, consent lasts a potentially long period of time. If I consent to marketing when I set up a direct debit, but later cancel the direct debit, it's sensible to refresh consent at that time. On the other hand, I have received marketing from some charities for years because I opted into it and I am still interested in their work. The crucial factor is the ability to unsubscribe. As with so much in DP, forward planning and transparency are your friends. If you know at the outset that you want to keep using data for an extended period, it's much easier to explain that and get consent for it.

Actually asked question: *Are we able to ask for lifetime consent rather than asking every couple of years?*
Answer: Arguably, yes you are. I suspect the ICO would argue that such an arrangement is not fair, but it's for you to make the case. If you were to say "we will send you marketing (or whatever you call it) until you tell us to stop", and a person willingly opted into that, I believe it would be compliant i.e. I do not think the ICO would enforce against it *if* the consent was properly and fairly obtained. The difficulty of getting freely-given, specific and informed 'lifetime consent' should not be overestimated.

4.10 GDPR and consent

Largely, the GDPR re-emphasises the Directive's requirements for freely-given, specific and informed consent. There are some important elements, some of them new. For one thing, GDPR consent must be 'unambiguous', and if that isn't enough to convince you that opt-out is dead, the recitals spell out that 'silence' or 'inaction' cannot be interpreted as consent. Just as important is the requirement that consent be 'demonstrable' – this doesn't kill off the idea of verbal consent but it does place a burden on the organisation to be able to provide evidence.

You can't bundle up consent with a service or action that is inherently separate – a classic bogus way of getting consent is 'by doing X, you consent to us doing Y'. X and Y must be inherently linked. A common example of this is making it a condition of receiving free Wi-Fi that the subject agrees to marketing. There is no consent here, because it's not freely given.

If you believe that you have consent to a GDPR standard, there is no need to renew it before May 2018. However, if you do not have consent, you will need to go back to the subject and obtain consent. The ICO position is that asking a person to opt into marketing when nothing else is going on is itself marketing – so if you email an existing donor or contact knowing that they have opted out or never gave consent in the first place, an email requesting / suggesting that they opt back in is essentially marketing. Although this is a somewhat circular argument, if you don't have consent to send a marketing email, you don't have consent to send an email asking the person to opt back in. The ICO fined Flybe and Honda in March 2017 for asking people to opt back in. The only valid way to contact the person is by post, or face to face if that opportunity arises.

Actually asked question: *Do prospect researchers need unambiguous consent to create profiles of potential donors?*
Answer: No, but the researcher needs to go through the process to justify using the legitimate interests condition instead, and the fairness provisions must still be satisfied.

Actually asked question: *Is it different for a charity to collate publicly available information to a private company that carries out similar research?*
Answer: No – if a private company is collating personal data and making profiles, the rules are exactly the same for them. An argument *could* be made that people might have higher ethical expectations of charities, but I don't believe that such an argument could survive scrutiny in an enforcement situation. The reason why charities have suffered the ICO's wrath is simply that the Mail exposed their practices, while other sectors labour under the radar.

Actually asked question: *what happens if you don't have good records of consent i.e. the person is on your database, but you cannot be certain that they opted into marketing? Can you contact them by email to ask if they still consent to receive marketing?*
Answer: it's a gamble. It's unlikely that ICO will issue you with a PECR CMP if you email people whose data you obtained legitimately to say '*we think we've got your consent to send you marketing, can you confirm if we are right*?'. However, lack of good consent records (especially if you don't know how you obtained the data) make life problematic to say the least. It's hard to argue that contacting people is compliant when you're contacting them because you haven't really been compliant, and failure to keep good records isn't very compliant.

The ICO's Direct Marketing guidance (para 74) makes clear that they believe you cannot email or text people to request consent for *future* marketing because that email or text would itself be marketing – if there is no evidence that you have consent, post is your only option.

4.11 Legitimate interests

The alternative to consent is legitimate interests. The full text of the condition is as follows: "*The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject*". There are a

series of hurdles to clear here – if you want to use legitimate interests instead of consent, you need to clear them all.

First, I think it's a safe assumption that raising funds for a charitable cause is a legitimate interest, understanding whether a person has the means to support such a cause is a legitimate interest, and assessing whether they would be likely to donate is a legitimate interest. I don't think this is controversial, if only because I don't think legitimate interest is a high bar to clear. Anything that isn't illegal, immoral or secret is likely to be a legitimate interest. Making a profit from a legal business is plainly a legitimate interest, so soliciting a charitable donation or other similarly philanthropic act must also be a legitimate interest.

Second, whatever it is you want to do – wealth screening, marketing, whatever else – must be **necessary**. The onus is on you as a charity or fundraiser to make a case – not prove, necessarily, but make a compelling case that your data processing is necessary. Look at how much of your income is derived from wealth screening, or the effect of its loss on your ability to carry out your objectives

Guidance for fundraisers issued by the Information Commissioner in 2017 says that profiling donors and potential donors isn't necessary for the straightforward process of administering donations, and should be treated as a distinct purpose. Given the extent to which wealth screening can involve creating a profile of an individual, assessing their financial situation, age, propensity for giving, there's logic to the assertion that it's not simply an admin matter. It is an assertion rather than a fact, and you can challenge it if you wish.

However, the argument they go on to make deserves a great deal more scepticism – they claim that many wealth screening techniques are intrusive and that "*[individuals] may not want their personal data analysed and profiled to assess how much they could donate*". Many fundraisers have argued that the ICO makes this argument without any evidence of what donors think, which is a valid criticism. The DPA doesn't say which purposes legitimate interests can be used for. The ICO is entitled to express their opinion, but the document is not binding. You would be a fool to ignore their view, but disagreeing with them is not forbidden. If you want to make a case that legitimate interests is an alternative to consent, make the case, but as I say throughout this document, make that case in advance.

Moreover, the practice that delegitimises wealth screening in this context isn't the failure of the legitimate interests condition, it's the fact that the process effectively happens in secret. If you accept the assertion is that donors might object, you can lessen the impact of this by offering donors the option of an opt-out or some other way to register an objection. The GDPR offers a straightforward right to object to

any processing based on legitimate interests, which means that any contentious processing under the condition will be subject to challenge anyway.

When Experian proposed a scheme called 'Rental Exchange', which involves information about rental payments being shared without consent from housing organisations to build up credit profiles, the ICO did not tell Experian that they could not use legitimate interests. I know this because I made an FOI request to the ICO and read their correspondence. There is an argument that the sharing is in a tenant's interests - some tenants have no credit history to speak of, and a record of consistently paying rent might help them to build one. However, Rental Exchange is a separate activity from the main business of the housing association, and some tenants could conceivably suffer disadvantages (like a worse credit record) as a result.

I think consent is the only acceptable option for Rental Exchange because it involves data sharing with a third party that is unnecessary for the primary relationship. The relationship between tenant and landlord is asymmetric, and relying on tenants opting-out when they may not understand and or even notice the data sharing is, to my mind, unreasonable. Nevertheless, if the ICO did not object to a use of legitimate interests to justify a disclosure for to a third party that would affect a person's credit record, I believe their objections over legitimate interests for wealth screening are unfounded, and worthy of challenge. To be clear, this document is not legal advice, but having watched the ICO for more than a decade, I don't believe that the ICO will enforce on this. This doesn't take away the problem of fair processing – that's the real problem here.

The final element of legitimate interests is *"except where the processing is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject*". This is vital. The legitimate interests condition is a balancing act – the legitimacy of your (or the third party's) interests balanced against the effect on the rights and freedoms of the subject. Under DP, legitimate interests falls if the effect on the subject is prejudicial; under GDPR, the bar is lowered. Prejudice is replaced by a simple balance – is your legitimate interest overridden by the effect on their rights and freedoms? Under either, the onus is on you to demonstrate that what you're doing is a legitimate thing to be doing.

Let's look at wealth screening in this context. Many fundraisers claim that especially when dealing with high net-worth individuals, a certain element of research is not only beneficial to the charity, but expected by the individual. The processing has to be fair and there is no escape from that. However, if the expectation argument is true, this builds a solid case for legitimate interests as an alternative to consent. This argument might work if your prospect is a busy millionaire who doesn't want to be

fussed with approaches that don't fit with their priorities. The RSPCA subjected seven million people to wealth screening. The high net-worth individual argument hits a brick wall at this point. You can make a sensible argument that legitimate interests works for specialised cases, but profiling millions isn't the same thing.

4.12 Sensitive personal data (GDPR special categories)

An additional complication comes if you are using personal data that DPA defines as sensitive, or GDPR defines as 'special categories'. The sensitive data categories are racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition; sexual life, the commission or alleged commission by the data subject of any offence; or any proceedings for any offence that are currently ongoing. If you want to use sensitive data as part of your fundraising, you cannot simply rely on the six conditions mentioned in section 4.5.

There are additional conditions in Schedule 3 of the DPA and Article 9 of the GDPR. They are tightly defined, making the use of sensitive / special categories personal data very difficult in any situation. Legitimate interests and contract do not appear in the additional conditions, and while consent is on the list, it must be 'explicit'. There is no small amount of debate in the DP community about the difference between 'unambiguous' and 'explicit' consent – I don't think that there is much meaningful difference between the two because the bar for unambiguous is set high enough as it is. It is highly likely that the only valid condition for processing sensitive / special categories is explicit consent.

4.13 Obtaining data from third parties

I quoted a sentence from the privacy policy of a Big Name Charity above. It's worth considering it again for one final fairness issue. They say, *"In order to ensure that the data we hold about you is accurate and up to date, we may occasionally use information sources that are in the public domain to verify your details, such as address and telephone number."*

There are legitimate sources for addresses (the open electoral register) and phone numbers (the BT phone disc, which includes all residential phone numbers that are not ex-directory). These sources don't cover everyone – I don't appear on either – but they are legitimate and the data has been fairly obtained. Using them won't undermine the fairness of your processing. If your data source is illegitimate, you cannot comply with the first principle. You are not obliged to obtain data directly from the subject, but compliance is more difficult when you don't. The onus is on

you to show that you have fairly obtained the data, which means you need evidence from the data supplier about when and how the data was obtained.

In 2015, I received unsolicited texts and emails from Optical Express, so I asked where they obtained my data from. The answer was MyOffers, a competition website company that used to go by the amusingly on-the-nose name of 'Interactive Prospect Targeting'. In 2011, I used my DP rights to stop MyOffers from trading or sharing my personal data; by obtaining my data from them, both Optical Express and MyOffers automatically breached DP. MyOffers also sold my data to the Claims Advisory Group, Digitonic (a marketing firm), and Experian, none of whom contacted me to tell me that they had received my data, although all confirmed they wouldn't use it when I contacted them.

I asked MyOffers why they were selling my data, and they claimed I had opted in when filling out a survey run for them by a third party. They assumed that the third party had obtained my consent without actually seeing any evidence. I asked the third party company how they had obtained my data, and it turned out that *another* company had run the survey on their behalf. Needless to say, I had no memory of completing the survey, while the only evidence of my consent the company at the end of the chain could offer was the IP address of a computer in Stoke.

Optical Express lost an appeal against an ICO enforcement notice at the Tribunal in 2015; the Tribunal decided that it was impossible for Optical Express to obtain consent to send marketing messages via a third party as they claimed. One recipient of the texts had filled in a questionnaire with Thomas Cook that made no reference to Optical Express, or even eye treatments. The Tribunal sums up the effect of a failure to process data fairly in this situation: *"when a data subject gives consent they must be informed about the processing to take place, including who by and what for. In no other way can consent be said to be "informed…. in order to ensure that the processing is fair you must tell the data subject (a) who is going to process the data, (b) what it will be processed for and (c) anything else at all to ensure fairness, such as, to whom the data might be passed and any applicable rights which the data subject has in relation to the processing"*

More recently, in November 2016 the claims management firm Quigley and Carter lost an appeal against a monetary penalty for sending spam texts after claiming to have been let down by the companies who supplied them with data. Another marketing company (Media Tactics) was fined by the ICO in March 2017. The monetary penalty notice in Media Tactics' case discusses the sources of personal data they used. It says "*Some provided a long list of general categories of*

organisations to whom the data would be disclosed, including for example the following sectors: astrology, charitable organisations, comparison websites, debt collection, financial providers, fashion and leisure goods, gambling, general retailers, household goods and services, insurance providers, shares, health and welfare, legal services, subscription services, mobile telecommunications, and general marketing." The notice goes on to say "*Informing individuals that their details will be shared with unspecified third parties, is neither freely given nor specific and does not amount to a positive indication of consent*".

The onus is clearly on the data controller to ensure that they have consent, and that data that they obtain is fairly obtained. If you obtain data from a third party, and the source is not self-evidently legitimate (a self-evidently legitimate source is the BT phone disc, rented from BT), you should assume that it has not been fairly obtained until you see the evidence that it has. Assurances from the data supplier are not enough; you need evidence that the data is what they claim it to be.

An organisation that shares or sells data to you is a data controller, but you become the data controller for it once it is received. You cannot claim innocence or ignorance if it turns out that the data is stolen, or the supplier has misrepresented the purposes for which it was obtained. Even if the supplier lies to you ('opted-in' and 'fully consented' are two lies to look out for), once you process the data, you are responsible for its flaws. If the salesman told you that the subjects consented and this turns out to be a lie, if you failed to obtain evidence of the consent before you bought the data, the ICO is entitled to enforce on you. It's like buying stolen goods – ignorance is no defence.

4.14 Suppression lists

To comply with a variety of different Data Protection and PECR requirements, you need a suppression list. This is a list of all the people who have told you that they do not wish to hear from you. It is reasonable to split your suppression list into different channels, but only if the person has made a nuanced request (i.e. you can mail but not phone).

A person should be on your suppression list if they formally exercise their rights under Section 11 of the Data Protection Act, which allows them to stop marketing no questions asked, or for them to tell you not to start. This is a useful tool for the individual, as they can use Section 11 to say that even if you buy data from a third party (a third party who may be selling that most bogus of commodities, the 'opted-in list'), because they are already on your suppression list, you will not contact them. The suppression list will naturally include people who use the Fundraising

Preference Service, once it is up and running – at the time of writing, the FPS appears to be a service which will allow people to opt-out charity by charity.

Whenever you carry out any form of contact that counts as marketing, you will screen people against that list.

Actually Asked Question: *Would the creation of very basic records in our database without explicit consent be OK under legitimate interest as a means of ensuring that we don't contact people with do not wish to be contacted?*
Answer: Yes, legitimate interests would apply - however the fact that the person has given you their details for suppression purposes allows you to base the processing on consent anyway.

4.15 The Right to Be Forgotten under GDPR and suppression lists

Several people have asked me on various training courses whether the Right to Be Forgotten will complicate suppression lists. I do not believe that it will, for two reasons. First, if a person wants to be on your suppression list, they will not ask you to delete the data you hold on that list. If they insist that all of their data is deleted, you can point out that by complying with that request, you will be unable to comply with their request to be on your suppression list; they cannot have both and will have to choose which is more important to them.

Second, the Right to be Forgotten has certain safety valves – expunging every reference to a person is a very different undertaking to removing specific facts. For a request that is manifestly unfounded because it is excessive can be refused or at the very least, it can attract a charge. I think many people will want to use the right to be forgotten to remove outdated, irrelevant or excessive information – they will not want to have their presence on your suppression list to be deleted.

4.16 Profiling under the GDPR

A significant change coming from the GDPR is the stricter controls on what the GDPR calls 'profiling' – the use of automated techniques to "*evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*". Essentially, this is the use of machine or computer-based analysis or decision-making – the creation of a profile isn't enough to trigger the GDPR's requirements, it needs to be done using a computer program or similar technique.

The DPA is concerned with purposes, but here the GDPR focusses not just on purpose, but on the technique used. Several things are required once profiling is being undertaken:

- individuals need to be informed that decisions affecting them are being taken using profiling (art 13 & 14)
- they have a right to challenge the use of profiling, especially where the justification is legitimate interest (Art 21) and to demand the opportunity to make representations and for human intervention (Art 22)
- impact assessments have to be carried out where profiling will have significant legal effects on the individual (Art 35)

It's impossible to know how these provisions will work out until the GDPR is in force and people attempt to use their rights. Nevertheless, it's worth considering now whether analysis is being carried out and decisions are being taken using machines, rather than humans.

Actually asked question: *The database team use an score (how recent was last donation, frequency of donations, monetary value of donations) to rank 1000 donors on our database. Does this count as profiling under the GDPR?*
Answer: It depends if people manually work this out, or if a computer carries out the analysis – if the computer does it, it's profiling.

5 PECR

If this guide has any real purpose, it is to persuade you to delve into the complexities and grey areas of Data Protection and develop your own take on how it works for your organisation. This last section, by contrast, is a model of simplicity, because it is about PECR. PECR is an additional layer of law that applies solely to the delivery mechanism of direct marketing. PECR is not about principles or subtlety. It is about RULES.

It's worth remembering that one of the few unambiguous rules in the DPA is in Section 11, which gives people a right to opt-out of any direct marketing, or request that it does not start. The GDPR contains an almost identical provision in Article 21. Whatever justification you use to send direct marketing, you have to stop if the person asks you to.

5.1 What is marketing?

In 2016, Stephen Lee, an academic and former fundraiser was reported as having attacked the Information Commissioner's Office for their interpretation of direct marketing at a fundraising conference. It was, he was quoted as saying "outrageous" that the Commissioner's direct marketing guidance stated that any advertising or marketing material that promoted the aims and ideals of a not-for-profit organisation was covered by Data Protection. According to Lee, only fundraising activities should be considered to be marketing. Third Sector quoted him as saying "*Who says that's right? Just the ICO. Who did it consult? No one.*" and went on to say "*Why and how and in what way should we be compelled to comply with that proposition?*"

I wasn't at the conference in question, and Mr Lee's comments may have had nuance that was lost in translation. Nevertheless, the question deserves an answer – is information that promotes the organisation's aims and ideals covered by the definition of marketing in the way the ICO says it is? The short answer is yes (if you accept the ICO's view, you can skip the text in italics below!

The long answer can be found by looking at a number of different perspectives that have been brought to bear on the issue of marketing since DP's inception.

1) The Council of Europe

In 1985, the Council of Europe issued a Recommendation on the protection of personal data used for the purposes of direct marketing. The definition of direct

marketing includes both the offer of goods or services and "any other messages" to a segment of the population.

2) The 1995 Data Protection Directive

The Directive makes clear that direct marketing rules apply equally to charitable organisations and political parties as they do to commercial organisations, and emphasises the need for people to be able to opt-out of direct marketing.

3) The Data Protection Act 1998

Section 11 of the Act states that the definition of Direct Marketing "the communication (by whatever means) of any advertising and marketing material which is directed at particular individuals". The important word there is "any" – organisations do not get to pick and choose which of their promotional messages are covered and which are not.

4) The Privacy and Electronic Communications Regulations 2003

PECR sets up the rules for consent over electronic direct marketing (consent for automated calls, opt-out and TPS for live calls, consent for emails and texts). It does not define direct marketing, but instead says this "Expressions used in these Regulations that are not defined in paragraph (1) and are defined in the Data Protection Act 1998 shall have the same meaning as in that Act". Therefore, the DPA definition applies to PECR.

5) The Information Tribunal (now the First Tier Tribunal)

In 2005, the Information Commissioner served an Enforcement Notice on the Scottish National Party after they repeatedly and unrepentantly used automated calls featuring Sean Connery to promote the party in the General Election. The SNP appealed, and in 2006, the Information Tribunal considered the issue. One of the main elements of the SNP appeal was against the ICO's definition of direct marketing. Although the case is about a political party, the ICO's submissions are based on the proposition that charities as well as political parties are covered by the definition of direct marketing, and that the definition cannot be restricted to fundraising alone. The Tribunal accepted the ICO's view in full, and dismissed the appeal.

Having overcome that hurdle, the next question is what the rules actually are. The PECR rules cover different channels for electronic marketing, and are as follows:

5.2 LIVE CALLS (Reg 21)

SHORT ANSWER: consent or legitimate interest if they are not registered on the Telephone Preference Service; if they are registered on TPS, you can't call them unless they specifically tell you that you can.

LONG ANSWER: you can make live unsolicited calls unless the number is on the TPS or the person has told you that you can call them. A person can therefore override their TPS membership and tell you that you can call them, but this has to be active. You have to allow people to opt-out during the call itself, so your agents or call-centres have to be geared up for this. You cannot tell them to contact you separately after the call.

You cannot call a number registered on the Telephone Preference Service unless the person who pays the bill has told you that you can. The fact that a person using that number has previously made a donation is irrelevant. The fact that you may have used some opt-out / squeaky fine-print is irrelevant. Consent means that the person voluntarily said "You Can Call Me". If you don't have that, you can't call them. You cannot interpret a separate action as consent – only 'yes, call me' is consent.

If the person is not on TPS, then using an opt-out system is acceptable, although you must remember that all other parts of Data Protection still apply. If you have not obtained the data fairly and lawfully in the first place, you won't be able to rely on legitimate interests.

Making live calls requires you to have access the up-to-date TPS list, either by renting it direct from the TPS, or paying someone who has access to the TPS list to screen your numbers against the list. You cannot make marketing calls without accessing TPS data unless you are calling people that you know have consented to receiving your calls. Buying numbers of so-called 'opted-in' individuals from a third party is a naïve and risky step to take in any context, but especially this one.

Actually asked question: *what happens if someone registers with the TPS after they have given consent? Can we contact them to clarify?*
Answer: If the person has given freely given, specific and informed consent for marketing, a subsequent TPS registration does not cancel this out. You can call a person who has *specifically consented* even if they then join the TPS. In this situation, they would need to contact you directly to opt-out of calls. Of course, this consent could not be an opt-out or an inferred consent like the scenario where a person has donated or bought a raffle ticket and this is interpreted as consent (it isn't).

5.3 AUTOMATED CALLS (Reg 19)

SHORT ANSWER: You can only make automated calls to those who have consented

ALTERNATIVE SHORT ANSWER: Don't use automated calls because they are the hallmark of the spammer

LONG ANSWER: Regulation 19 separates the use of automated calls from other phone calls dealt with under Regulation 21, so the use of automated calls for marketing purposes has different rules. You can only make automated calls to those who have specifically said 'I would like you to ring me with recorded direct marketing messages'. It is exceptionally unlikely that anyone would consent to this, so the great majority of automated marketing calls are unlawful. Screening the numbers against the TPS is irrelevant in this context so there is no benefit to doing so. It's consent only, with all the difficulties that obtaining consent implies.

Separately, it's worth thinking about the nature of automated calls. They can be distressing and confusing for vulnerable people. Many companies that use automated calls are involved in claims management, making millions of automated calls cheaply just to identify a few likely prospects, annoying huge numbers of people in the process. Automated calls are often pile-it-high, sell-it-cheap marketing; persuading people to receive calls of any kind is the only safe way to go.

5.4 EMAIL / SMS: (Reg 22)

SHORT ANSWER: You can only send texts and emails to those who have consented

SHORT ANSWER FOR BUSINESS / PROFESSIONAL EMAILS / TEXTS: You can use consent or legitimate interest

You can only send text marketing to individuals with consent. PECR gets its consent rules from the DPA, so this means freely given, specific, informed active consent for

texts. A popular way to initiate text marketing is the "Donate £3 to Prevent the End of The World" technique. In the small print on the poster or advert, there may be a squeak about opting out. This is not consent. If you send texts to someone who has not clearly ticked a box, or entered their number in a box which clearly states that by "entering the number, you will receive marketing", you can't send the texts and you are breaching PECR if you do.

PECR distinguishes between two sorts of recipients, however. The above rules apply to 'individual subscribers' i.e. accounts provided directly from a mobile or internet service provider to a customer. There is a second definition of a 'corporate subscriber' – this is where the account is allocated to the individual by an employer, educational institution or similar organisation. The rules in Regulation 22 apply only to individual subscribers. So-called business-to-business email is exempt from the consent rules in PECR, subject to the opt-out that every person has a right to under DP S11 and GDPR Art 21.

I am an individual subscriber for my email address timturnerspam@gmail.com, so you need to get my consent before sending marketing to me. The email address tim@2040training.co.uk would be considered to belong to a corporate subscriber, so you could send me unsolicited emails, but I would be able to opt-out using my DP rights. Arguably, the email address mail@2040training.co.uk would not be personal data, but here is a question – the fact that you might be able to send email to that final address, and technically they might not be able to opt-out, do you really want to be the kind of organisation that sends marketing after the recipient has told you to stop?

Actually asked question: *do we have to include an opt-out / unsubscribe option in our marketing emails?*
Answer: Unless you are relying on the soft opt-in (see below), you do not need to do this, although it is unquestionably good practice. You must provide a valid address via which a person can send an opt-out should they wish to.

Actually asked question: *can we use opt-out tick boxes for SMS and email?*
Answer: only if the recipient is a corporate subscriber – otherwise, consent for marketing has to be opt-in

Actually asked question: *can I use a business email to contact an alumni to ask them to reconnect with their university?*
Answer: yes (in the sense that you don't need consent) but that's one question answered. Other pressing questions include how you obtained the email address, and whether people would expect to receive emails from you.

5.5 THE SOFT OPT-IN

Regulation 22 includes the soft opt-in, a specific provision to allow for an opt-out approach for email and text in certain limited circumstances. It is sometimes referred to erroneously as the 'existing customer' exemption (even the ICO falls into this trap sometimes). The way the soft opt-in works is as follows:

- You obtain the email address / mobile number during a sale or negotiations for a sale – the language here is unambiguously commercial and there is no scope for interpreting a donation as a sale
- You give the person an opportunity to opt-out at the point of obtaining the data
- You send them emails or texts about similar products or services to the one they bought / were looking at when you obtained their details
- You give them an opt-out opportunity in every message you send to them

This is narrow and in most cases, does not apply to fundraising. Of course, you may sell products, raffle tickets or other similar items, in which case the soft opt-in would apply to you – but the only messages you could send would be about similar products to the item they purchased.

Actually asked question: *why can't we use the soft opt-in as charities? It seems very unfair.*
Answer: Charities can use the soft opt-in when selling products and services, just not when receiving donations. This is solely because of the way PECR is drafted. It's not particularly fair, but that's the problem with PECR. If it was principles-based, a donor / charity relationship might compare favourably with a customer / company relationship. But PECR is rules-based.

6 WHAT ELSE?

Once you have overcome the first and second principles, there is much else to do. Other principles require you to ensure an adequate level of personal data, ensure that personal data is accurate for the purposes you obtained the data for, set out retention periods, respect people's rights and keep data secure.

The eight principles are:

Second principle - personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Third principle: personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Fourth principle: personal data shall be accurate and, where necessary, kept up to date.

Fifth principle: personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Sixth principle: personal data shall be processed in accordance with the rights of data subjects under this Act.

Seventh principle: appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Eighth principle - personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

GDPR retains all of these elements – principles 1 – 5 are more or less the same, the 7th principle becomes the 6th, while rules over rights and international transfers are retained, although the rights are expanded.

When considering the rest of the eight principles, the rules for fundraising are substantially the same as they are for any other organisation. The things you have to do – especially around adequacy, reuse of data and retention periods – are driven by the purposes for which you use the data. The DPA and GDPR do not dictate time

periods or quality processes – the Data Controller must decide. I could pontificate about how much data you really need to do your work, but each individual organisation probably knows better.

As well as all that, there are rights of access, a right to have information corrected and right to sue for compensation. Under GDPR, there is the famous Right to be Forgotten, a new right whose effect is difficult to predict, and rights of portability and objection. Moreover, there is the obligation to keep data secure which, until the fundraising crisis, was the area of Data Protection most likely to result in enforcement action.

Once you're actually using the data, there is a lot more to think about. However, this is where this guide ends.

Good luck!

Acknowledgements

In 2016, several people working in charities sent me questions that they wanted the answers to. Those questions appear in this guide, and I would like to thank all of them for their kind assistance. A variety of accidents and mishaps delayed this guide's publication, but at the very least, I hope it is helpful to them even after all that.

I would also like to thank those charity and fundraising people who have interacted me with me on Twitter after my various blogs and other interventions into the charity sector, even though some of them were plainly just annoyed with me for being such a smartarse. This is not an unreasonable reaction.

Rowenna Fielding and Jon Baines took time out of their busy schedules to read a draft version of the guide, and I am immensely grateful for their time and comments, which made the difference between me abandoning the whole thing in despair and finally publishing it. This should not be taken as an endorsement of the guide, for which I bear sole responsibility.

About me

My name is Tim Turner. I have been working on Data Protection and Information Rights since 2001, when I got a job at the Information Commissioner's Office. I was working in a local authority library at the time and I blagged my way through the interview, chiefly motivated by the wish to get off the short-term contract I was working under. I did not want to become a Data Protection specialist, I just wanted a permanent job.

My time at the ICO was relatively short and undistinguished but it made my mind up that I wanted to work on information rights rather than catalogue Catherine Cookson books. Since then, I have been a Data Protection officer in two different councils (Derbyshire and Wigan) and an NHS body (the now defunct Manchester Primary Care Trust). In 2006, a training company asked me to do some courses for them because they had seen me speak at a conference, and my employer at the time (Wigan) graciously allowed me to do so in my spare time. This arrangement continued until I was working in the NHS, and the organisation I was working for was effectively abolished by the coalition government.

Since 2011, I have been a full-time trainer and consultant for myself and for several training organisations. Because I don't have an employer to embarrass, I write a noisy and provocative blog about Data Protection and I tweet disrespectfully about data protection and privacy issues. You don't have to agree with me about anything I say on those platforms, and you don't have to agree with the content of this guide.

I hope you have enjoyed reading this and have found it useful; if you think it would have been worth paying for, making a donation to any mental health charity would be a lovely gesture that I would greatly appreciate.

If you would like training, advice or consultancy on Data Protection, please contact me using the details below.

2040 Training Limited, Suite 63, 792 Wilmslow Road, Didsbury, Manchester, M20 6UG
Email: tim@2040training.co.uk
Registered in England - Company Number: **6682698** – VAT Number: **155713606**